CLAIMS

1. A registration authority comprising:

a protocol converter coupled to receive messages from a router targeting a certificate authority, and to receive messages from the certificate authority targeting the router;

wherein the protocol converter is configured to convert the messages received from the router in accordance with a first protocol and convert the messages received from the router to a second protocol and subsequently communicate the converted messages to the certificate authority; and

wherein the protocol converter is further configured to convert the messages received from the certificate authority in accordance with the second protocol and convert the messages received from the certificate authority to the first protocol and subsequently communicate the converted messages to the router.

2. A registration authority as recited in claim 1, wherein the registration authority is independent of the certificate authority.

3. A registration authority as recited in claim 1, wherein the first protocol is a Simple Certificate Enrollment Protocol (SCEP) enrollment protocol.

4. A registration authority as recited in claim 1, wherein the second protocol is a Public-Key Cryptography Standards (PKCS) enrollment protocol.

5. A registration authority as recited in claim 1, wherein the registration authority conforms to the network Working Group Request for Comments 2459 standard.

6. A registration authority as recited in claim 1, wherein the messages received from the router comprise one or more of: a router enrollment message, a get certificate revocation list (CRL) message, a get certificate message, and a get certificate authority (CA) certificate message.

7. A registration authority as recited in claim 1, wherein each message received from the certificate authority comprises a response to a message received by the registration authority from the router.

8. A registration authority as recited in claim 1, wherein the router is unaware that it is communicating with a registration authority rather than directly with the certificate authority.

9. A registration authority as recited in claim 1, further comprising a transaction ID table configured to maintain a mapping of router transaction IDs received from the router to certificate authority request IDs received from the certificate authority.

10. A registration authority as recited in claim 1, further comprising a request hash table configured to maintain a mapping of certificate authority request IDs to hash values of the router requests.

11. A registration authority as recited in claim 1, further comprising a password table configured to maintain a valid password issued to the router.

12. A registration authority as recited in claim 1, further comprising a module configured to receive a request for a certificate of the certificate authority and, in response to the request, return a certificate of the registration authority.

13. A registration authority as recited in claim 12, wherein the registration authority is a dynamically linked library.

14. One or more computer-readable media having stored thereon a computer program that, when executed by one or more processors of a computing device, causes the one or more processors to perform acts including:

transmitting a request for an enrollment certificate for a virtual private network to a registration authority operating independently of a certificate authority.

15. One or more computer-readable media as recited in claim 14, wherein the computer program further causes the one or more processors to transmit additional requests regarding maintaining enrollment in the virtual private network to the registration authority.

16. One or more computer-readable media as recited in claim 14, wherein the computing device comprises a router.

17. One or more computer-readable media having stored thereon a computer program that, when executed by one or more processors of a registration authority, causes the one or more processors to perform acts including:

receiving, from a device, a first message in accordance with a first protocol;

generating, based on the first message, a second message in accordance with a second protocol;

sending the second message to a certificate authority;

receiving, from the certificate authority, a third message in response to the second message and in accordance with the second protocol;

generating, based on the third message, a fourth message in accordance with the first protocol; and

sending the fourth message to the device as a response to the first message.

18. One or more computer readable media as recited in claim 17, wherein the device comprises a router.

19. One or more computer-readable media as recited in claim 17, wherein the first message comprises an enrollment message.

20. One or more computer-readable media as recited in claim 19, wherein generating the second message comprises:

verifying that the first message has been digitally signed by the device;

decrypting the first message;

extracting a certificate enrollment request from the first message;

generating a certificate authority request including the certificate enrollment request and a subject alternative names extension; and

creating the second message by digitally signing the certificate authority request.

21. One or more computer-readable media as recited in claim 19, wherein generating the fourth message comprises:

extracting a certificate from the third message;

generating a response including the certificate;

encrypting the response; and

creating the fourth message by digitally signing the encrypted response.

22. One or more computer-readable media as recited in claim 21, wherein extracting the certificate comprises accessing a set of certificates corresponding to the third message.

23. One or more computer-readable media as recited in claim 21, wherein the computer program further causes the one or more processors to perform acts including:

extracting a certificate chain from the third message; and

including the certificate chain in the response.

24. One or more computer-readable media as recited in claim 19, wherein the third message comprises a certificate authority pending response.

25. One or more computer-readable media as recited in claim 24, wherein generating the fourth message comprises:

generating a pending response;

encrypting the pending response; and

creating the fourth message by digitally signing the encrypted pending response.

26. One or more computer-readable media as recited in claim 24, wherein the computer program further causes the one or more processors to perform acts, in response to the certificate authority pending response, generating:

a hash value based on the enrollment message;

a hash table entry mapping a pending response ID, corresponding to the certificate authority pending response, to the hash value; and

a transaction ID table entry mapping the transaction ID, corresponding to the enrollment message, to a pending response ID corresponding to the certificate authority pending response.

27. One or more computer-readable media as recited in claim 26, wherein the computer program further causes the one or more processors to perform acts including:

receiving an additional enrollment message from the device;

accessing the transaction ID table to obtain the pending response ID corresponding to the additional enrollment message; and

transmitting, to the certificate authority, a certificate request including the pending response ID.

28. One or more computer-readable media as recited in claim 26, wherein the computer program further causes the one or more processors to perform acts including:

receiving an additional enrollment message from the device;

generating a new hash value based on the additional enrollment message;

checking whether an entry in the hash table matches the new hash value; and

if an entry in the hash table matches the new hash value, then,

obtaining a pending response ID, from the hash table, corresponding to the new hash value, and

transmitting, to the certificate authority, a certificate request including the pending response ID.

29. One or more computer-readable media as recited in claim 26, wherein the computer program further causes the one or more processors to perform acts including:

maintaining the hash table entry in the hash table for a selected amount of time.

30. One or more computer-readable media as recited in claim 26, wherein the computer program further causes the one or more processors to perform acts including:

maintaining the transaction ID table entry in the transaction ID table for a selected amount of time.

31. One or more computer-readable media as recited in claim 17, wherein the first message comprises a get certificate revocation list (CRL) message.

32. One or more computer-readable media as recited in claim 31, wherein generating the second message comprises:

decrypting the first message;

verifying that the first message has been digitally signed by the device;

extracting a certificate serial number from the decrypted first message; and

creating, as the second message, a get certificate by serial number request.

33. One or more computer-readable media as recited in claim 31, wherein generating the fourth message comprises:

extracting a certificate from the third message;

extracting a certificate revocation list distribution point from the certificate;

obtaining a certificate revocation list based on the certificate revocation list distribution point; and

generating, as the fourth message, a response including the certificate revocation list.

34. One or more computer-readable media as recited in claim 33, wherein the certificate revocation list distribution point comprises a uniform resource locator (URL).

35. One or more computer-readable media as recited in claim 33, wherein obtaining the certificate revocation list further comprises retrieving the certificate revocation list from the certificate revocation list distribution point.

36. One or more computer-readable media as recited in claim 17, wherein the first message comprises a get certificate message.

37. One or more computer-readable media as recited in claim 36, wherein generating the second message comprises:

decrypting the first message;

verifying that the first message has been digitally signed by the device;

extracting a certificate serial number from the decrypted first message; and

creating, as the second message, a get certificate by serial number request.

38. One or more computer-readable media as recited in claim 17, wherein generating the fourth message comprises:

extracting a certificate from the third message; and

generating, as the fourth message, a response including the certificate.

39. One or more computer-readable media as recited in claim 38, wherein generating the fourth message further comprises:

extracting a certificate chain from the third message; and

including the certificate chain in the response.

40. A method implemented at a registration authority, the method comprising:

receiving, from a device, a get certificate authority certificate request;

generating a response including a certificate of the registration authority; and

returning the response to the device.

41. A method as recited in claim 40, wherein the device comprises a router.

42. A method as recited in claim 40, wherein the get certificate authority certificate request identifies a dynamically linked library (DLL) that is the registration authority.

43. A method as recited in claim 40, wherein the response comprises a degenerated message.

44. A method as recited in claim 40, wherein the response includes both a signing certificate of the registration authority and an encryption certificate of the registration authority.

45. A method as recited in claim 40, wherein the response further includes a certificate chain of the certificate authority.

46. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 40.

47. A method comprising:

receiving a request, from a requestor, for a password to be used by a device when communicating with a registration authority;

authenticating the requestor;

generating the password;

adding the password to a password table; and

returning the password to the requestor for use by the device.

48. A method as recited in claim 47, wherein the device comprises a router.

49. A method as recited in claim 47, wherein generating the password comprises generating a random number as the password.

50. A method as recited in claim 47, wherein receiving, authenticating, and returning include using Secure Sockets Layer (SSL) to maintain secure communication with the device.

51. A method as recited in claim 47, further comprising keeping the password active for a selected amount of time.

52. A method as recited in claim 51, wherein keeping the password active for a selected amount of time comprises marking the password as invalid after the selected amount of time.

53. A method as recited in claim 51, wherein keeping the password active for a selected amount of time comprises removing the password from the password table after the selected amount of time.

54. A method as recited in claim 47, further comprising:

receiving a request from the device, the request including a request password;

checking whether the request password is included in the password table; and

processing the request if the request password is included in the password table, otherwise rejecting the request.

55. A method as recited in claim 54, further comprising removing, if the request password is included in the password table, the request password from the password table.

56. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 47.